Cyber Security

KROHNE Academy „Automatisierungstechnik in der Prozessindustrie“

Stefan Ditting
2013

1. Zusammenhang von Safety und Security
2. Organisatorische Maßnahmen (Awareness)
3. Technische Maßnahmen (Defence in the Depth)
    1. PC-Schutz
    2. PES-Schutz
    3. weiteres z.B. Trennung

Cyber Security

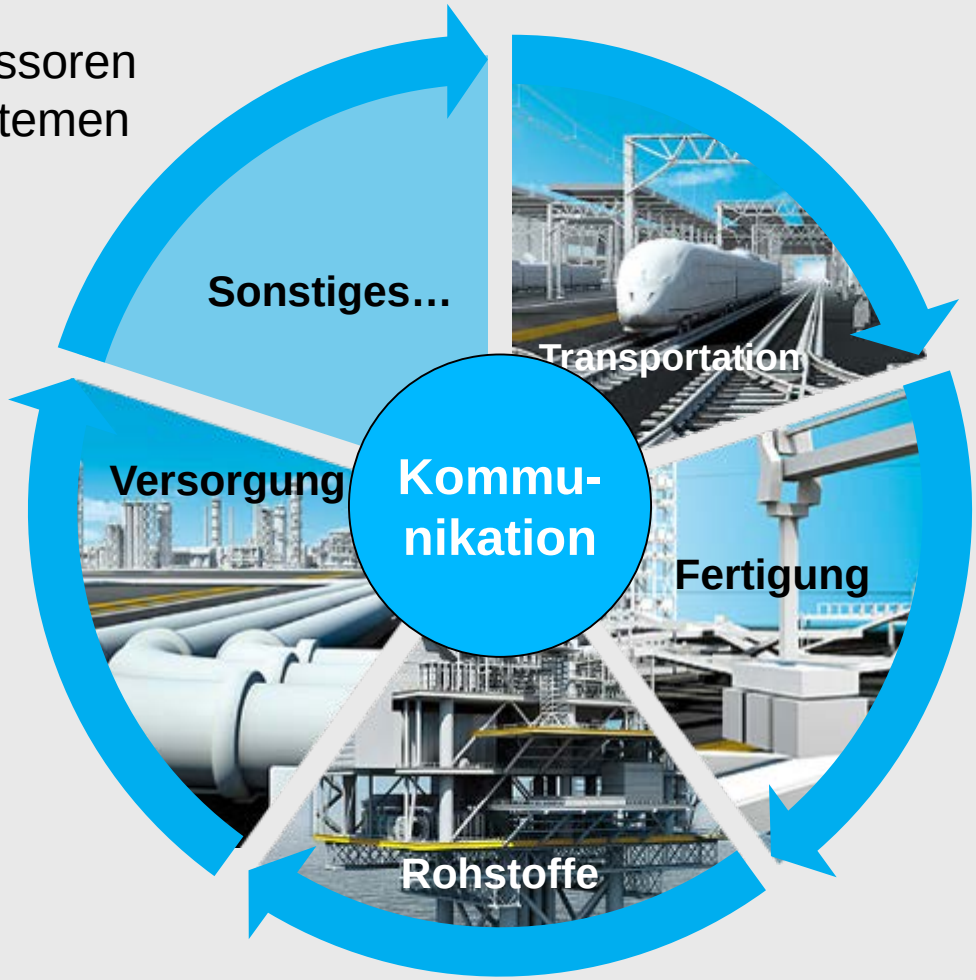
Agenda

Grundhaltung zur Security…

…dabei sind die Einschläge näher als sie meinen...

Automation: Eine Branche mit zentraler gesellschaftlicher Verantwortung !

>95% aller Prozessoren
in embedded Systemen



Sicherheit = Functional Safety + Cyber Security.

Functional Safety (Die Anlage darf keinen Schaden anrichten)

Menschen schützen

Maschinen schützen

Umwelt schützen

Cyber Security (Die Anlage muss vor Schaden geschützt werden)

Vertraulichkeit

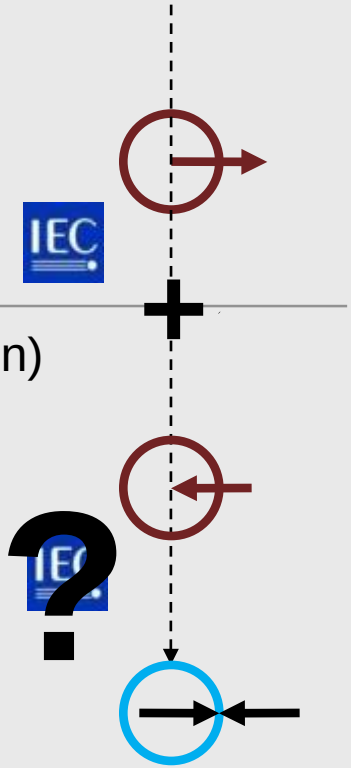
Verschlüsselung

Integrität

Signatur

Verfügbarkeit

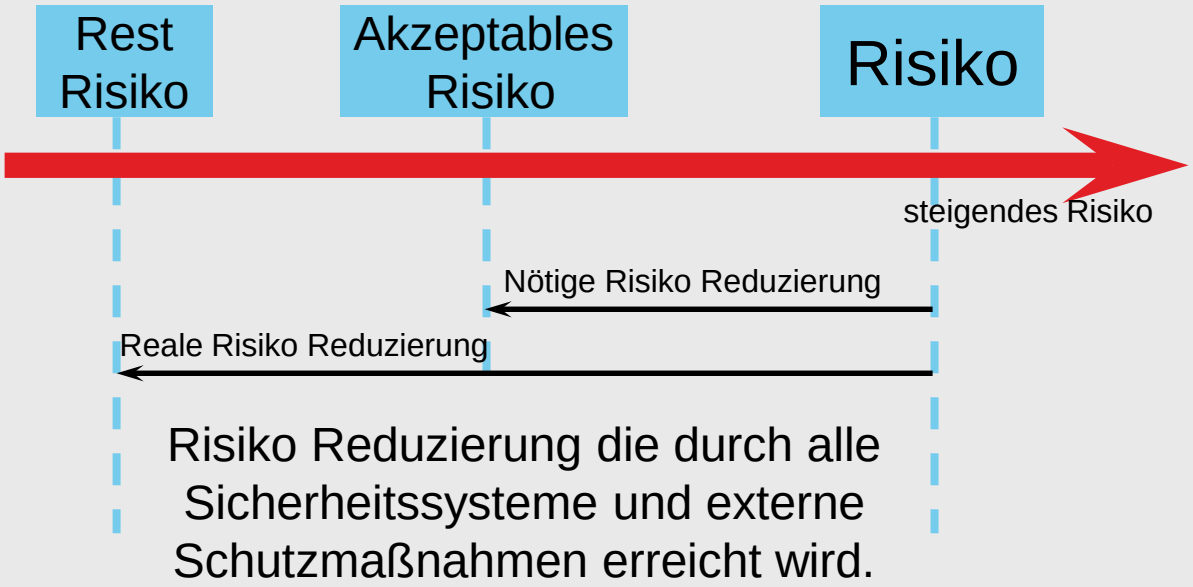
Trennung



Sicherheit

Es ist sicher zu stellen, dass **Information** und Daten (und damit auch **Programme**) ausschließlich für ihren **bestimmungsgemäßen Gebrauch** verwendet werden können und möglicher **Schaden** durch Verfälschung **vermieden** wird.

Risiken werden immer bestehen.

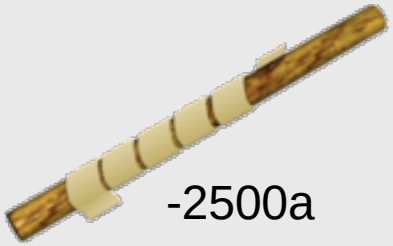


Safety: Risiko = (Unfallwahrscheinlichkeit) x (Schadensausmaß)

Security: Risiko = (Anfälligkeit x Bedrohung) x (Schadensausmaß)

? ? → **UNSICHERHEIT**

Sicherheit ist schon immer ein Grundbedürfnis.



-2500a

-500a

-70a

Zeit

Quelle: alle Bilder www.wikipedia.de

Mit der Skytale wurden von den Spartanern vor mehr als **2500 Jahren** geheime Botschaften **öffentlich** übertragen.

Grundkonzept Verschlüsselung:

01001011	Basis Text	10101101	01001011
11101110	Schlüssel	11101110	11101110
XOR	Operation	XOR	XOR
10100101	Encrypted Text	01000011	10100101

Wieder-holung

Die Methoden um Sicherheit zu gewähren werden seit Generationen verfeinert ….

… Genauso wie die Methoden diesen Schutz zu umgehen.

→ **Eine endgültige Lösung wird es <u>nie</u> geben !**

Historische Abriss von Security in der Automation.

HIMA bietet die 4te Generation von SIL4 hard wired safety Systemen an: PLANAR 4.
kein Netzwerk, keine Programmierung

1997 Markteintritt von HIQuad. SIL3, hohe Verfügbarkeit und safe**ethernet**.
Getrennte Netzwerke, SIL3 Programmierung

2001 Markteintritt HIMatrix. SIL3, klein, schnell, verteilt via safe**ethernet**.
Integrierte shared Netzwerke, SIL3 Programmierung

2008 Markteintritt HIMax. SIL3, NONSTOP, extrem schnell, verteilt via safe**ethernet**.
Integrierte shared Netzwerke, SIL3 Programmierung

Offenheit, Flexibilität

Robustheit

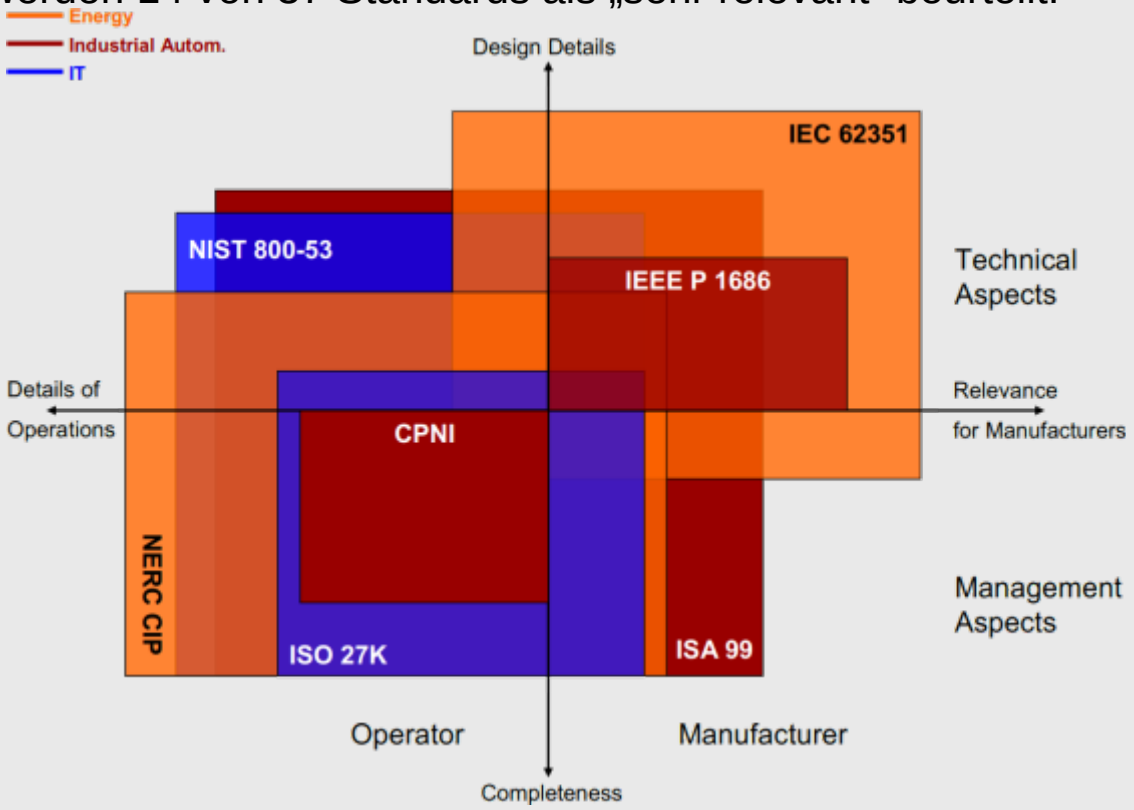
Industrie 4.0

So isses…

source: http://xkcd.com/927/

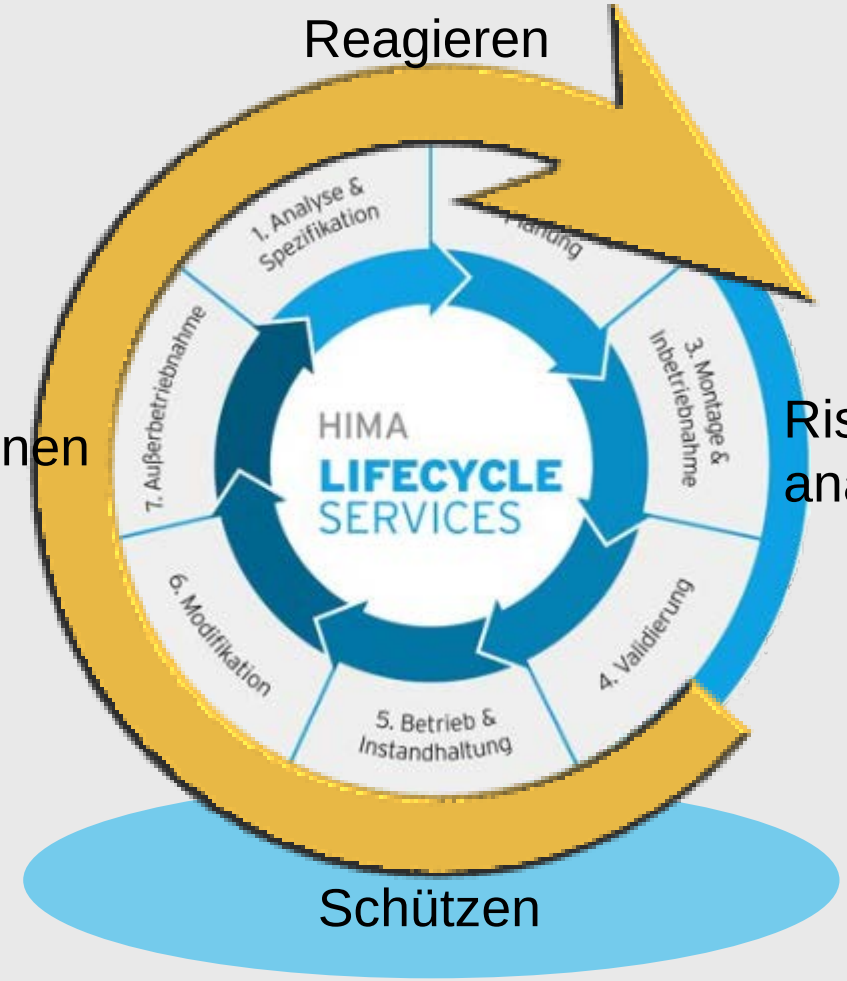
ESCoRTS

Für Betreiber werden 24 von 37 Standards als „sehr relevant“ beurteilt.
Für Hersteller werden 14 von 37 Standards als „sehr relevant“ beurteilt.



Quelle: http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Pages/FG-ESCORTS.aspx

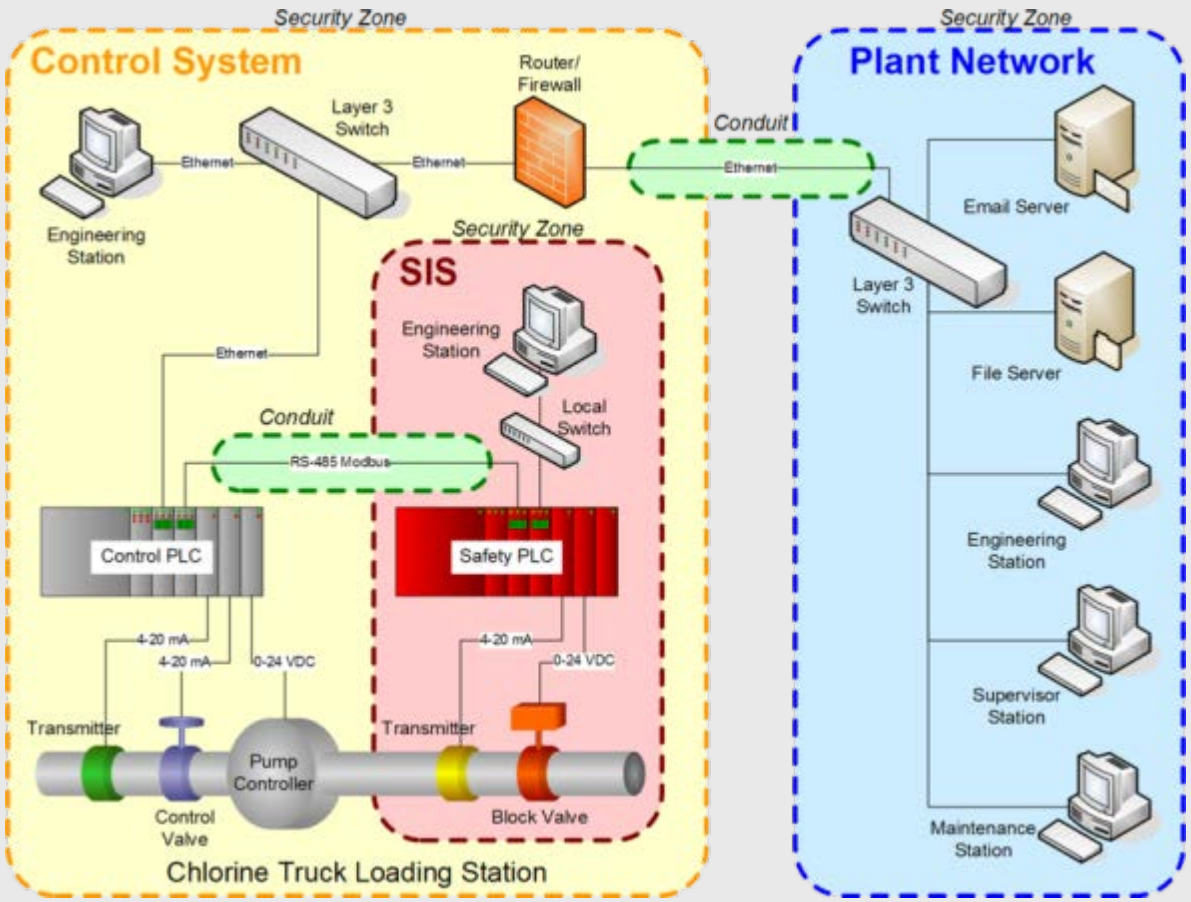
Security ist ein Prozess. (Plan, Do, Check, Act)



Security ist ein **Prozess** der das **Risiko** von Schäden durch externe Einflussnahme **reduziert**.

Dieser Prozess kann durch technische Maßnahmen, unterstützt werden.

Aufteilung in Zonen.



Quelle: ISA-99.03.03 Draft

Sowohl die IEC 61511 (Safety) als auch der Draft der IEC 62443 (Security) fordern Systeme in mehreren **Schutzebenen** aufzubauen. (Defense in the Depth)

SAL – Security Assurance Level

Wie bei Safety Integrity Level (SIL) wird versucht die Security zu quantifizieren. Zur genaueren Darstellung wird ein Vektor erstellt anstelle eines Wertes.

Bsp: SAL-T(Control Zone) = {2 3 1 3 4 3 2}

- SAL-T … Target
- SAL-D … Design
- SAL-A … Achieved
- SAL-C … Capabilities

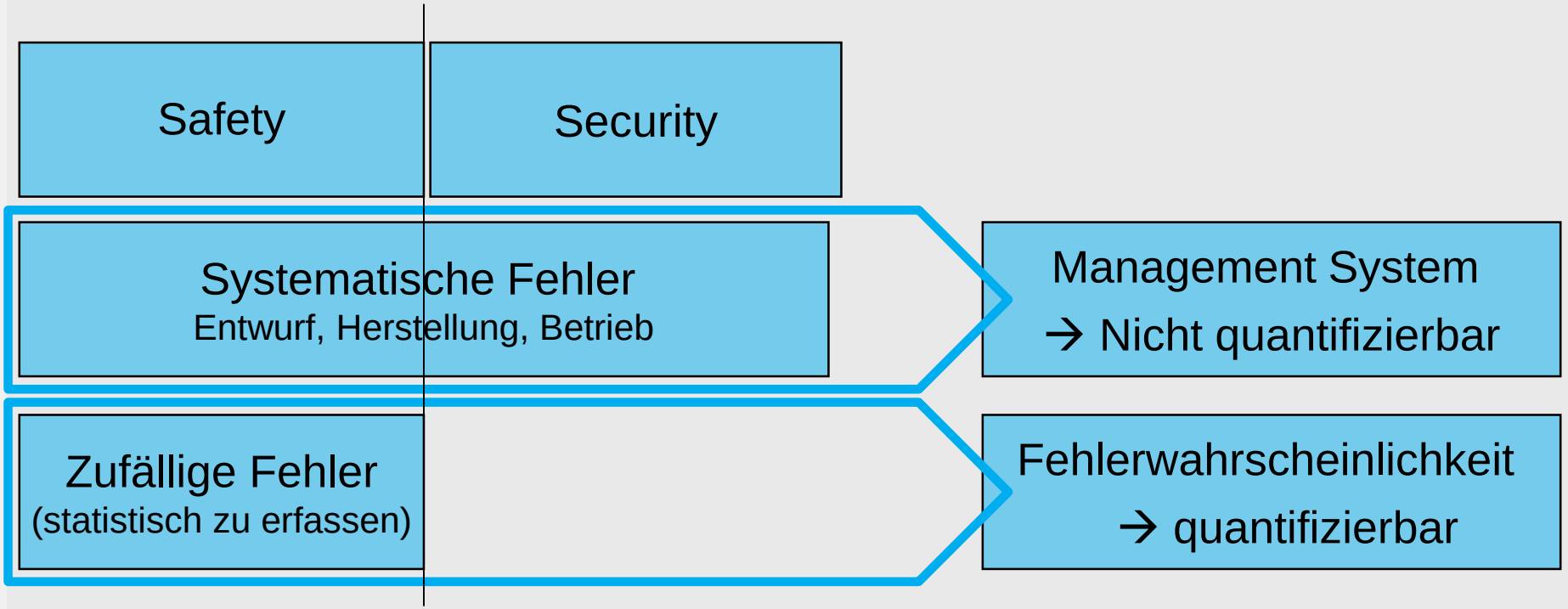
- SAL1 ... casual, coincidental
- SAL2 ... simple
- SAL3 ... sophisticated
- SAL4 ... extended

RA …… Ressource Availability
TRE …. Timely Response to an event
RDF …. Restrict Data Flow
DC …… Data Confidentiality
DI ……. Data Integrity
UC …… Use Control
AC …… Access Control

→ Keine exakten Bewertungskriterien wie bei SIL (Statistiken)
→ Zeitlich beschränkte Aussagekraft

Beschreibung SAL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=906330

Fehlerbetrachtung für Safety und Security.



→ Statistiken können lediglich für zufällig auftretende Ereignisse (Fehler) angewendet werden. Bei systematischen Fehlern sind **Statistiken ohne Aussagekraft**.

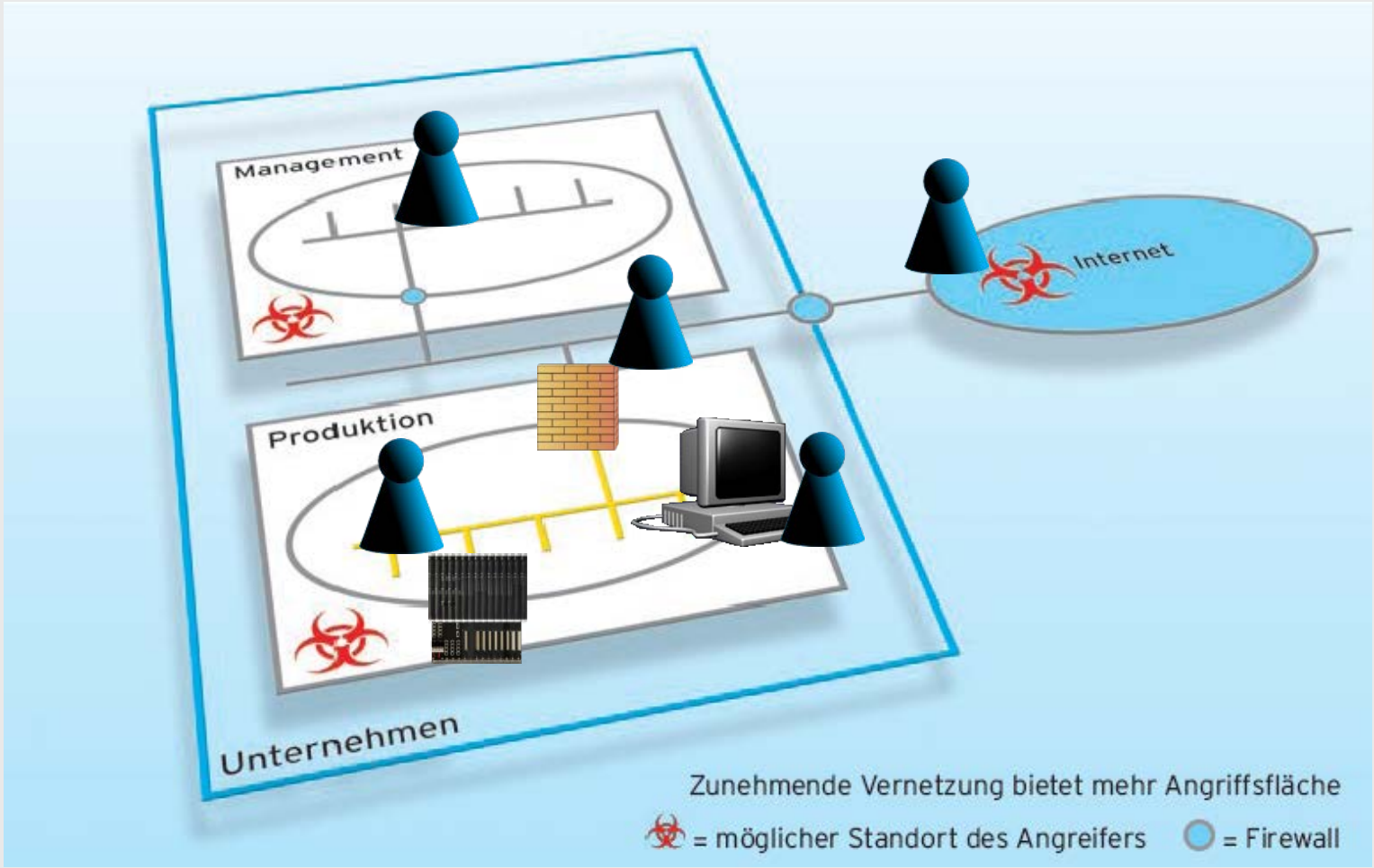
→ Management und Dokumentation können Security verbessern.

Was tun?

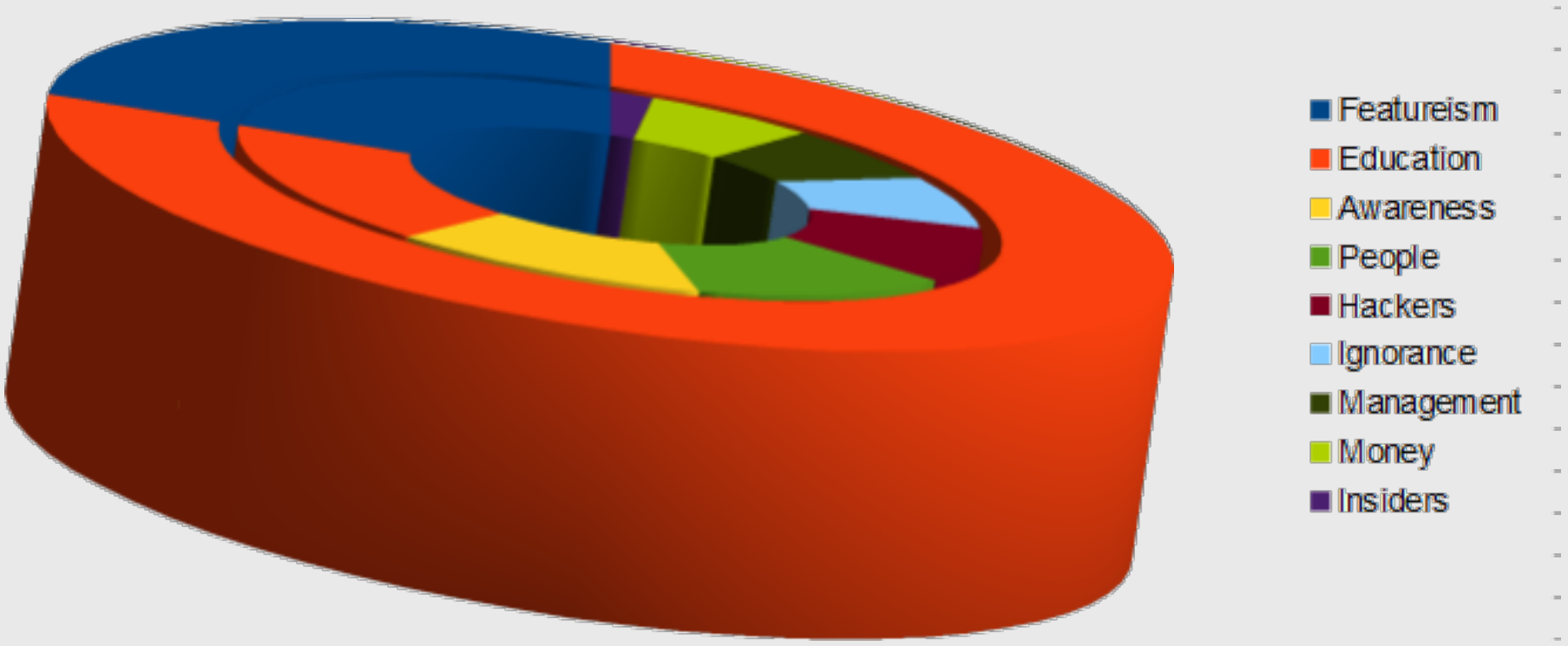
Orientierung an den existierenden Möglichkeiten:

1. Organisatorische Maßnahmen
   →Awareness
2. Technische Maßnahmen
   → Defense in the Depth
   1. PC-Schutz
   2. PES-Schutz
   3. weiteres z.B. Trennung

Umfeld.


Management
Internet
Produktion
Unternehmen
Zunehmende Vernetzung bietet mehr Angriffsfläche
= möglicher Standort des Angreifers
= Firewall

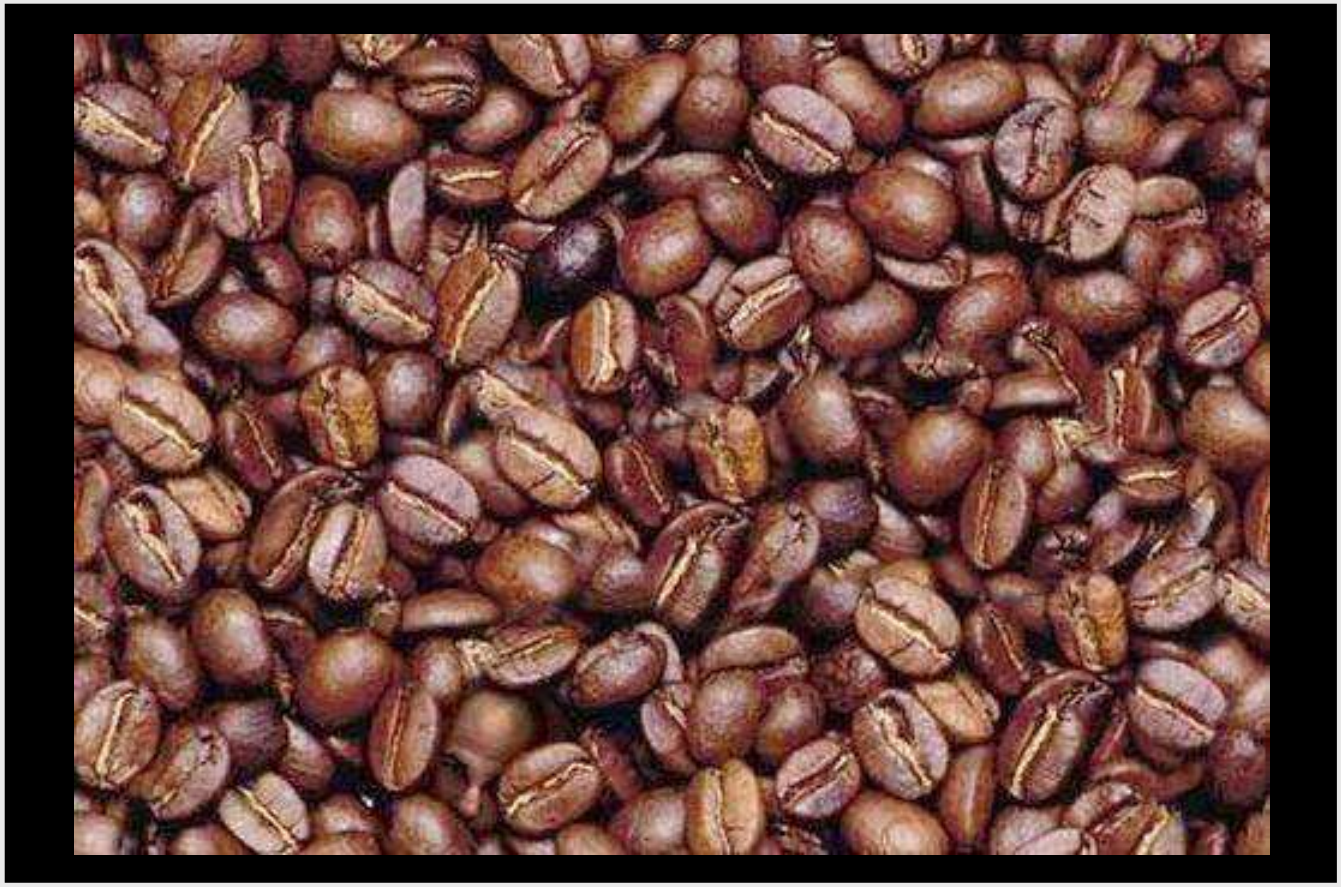
Eine Umfrage auf LinkedIn (Juli 2012)



24% technische Aspekte

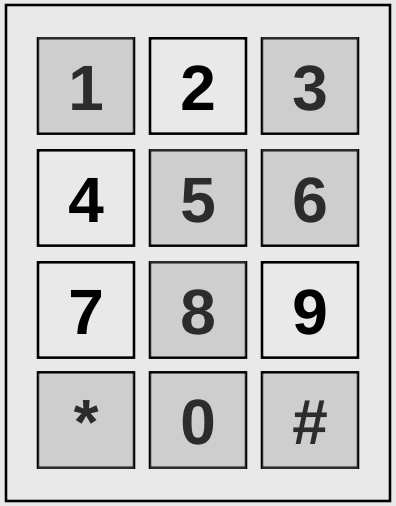
76% menschliche Faktoren

Bewusstsein schaffen !



Bewusstsein schaffen !

Menschen machen Fehler.



1. Ein Zahlenschloss an einer Tür bietet unendlich viele Möglichkeiten.	n = • t = •
2. Da der Code verwendbar sein soll wird er in der Länge begrenzt.	n = < • t = ?
3. Bediener sollen wissen ob die Eingabe akzeptiert wurde. Daher ertönt bei jedem Druck ein akustisches Signal.	n = 4 t = 20736
4. Die nicht benutzten Tasten werden im Laufe der Zeit grau.	n = 4 t = **24**

Menschliche Kreativität ist das Problem und die Lösung.
→ Kommunizieren sie die Eigenschaften der verwendeten Systeme!

Wie können dann 4stellige PIN sicher sein ??

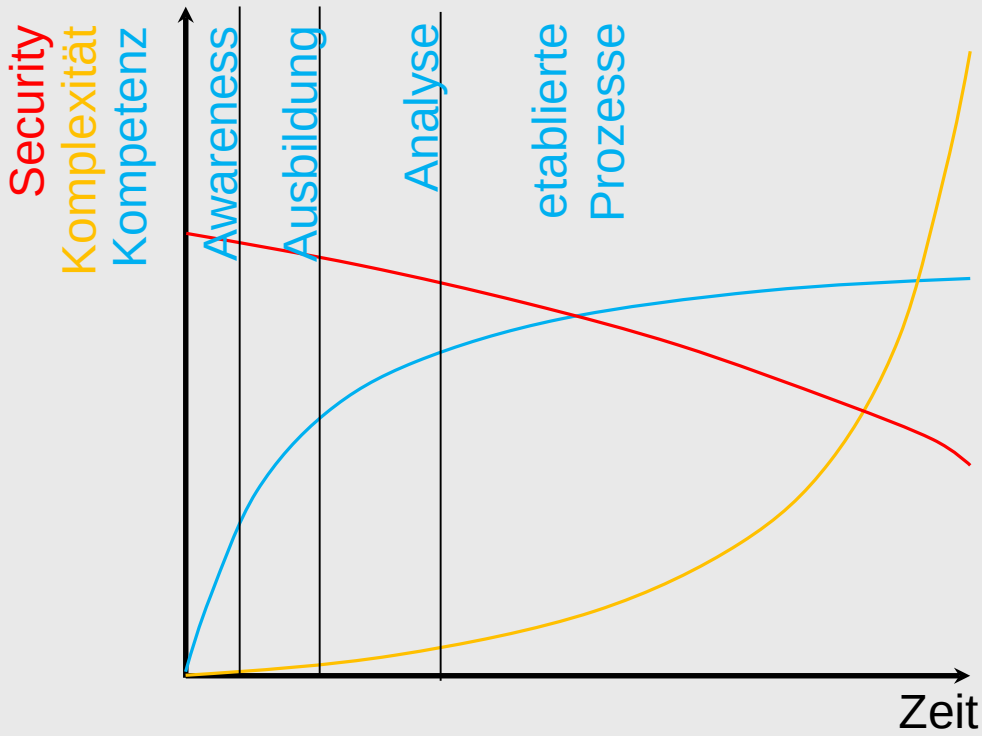
- Nach 3 Fehlversuchen wird die Eingaben gesperrt.
- **Es gibt keine universelle Lösung, sondern es müssen immer die individuellen Umgebungs-bedingungen betrachtet werden.**
- Übrigens: die häufigsten PIN (>20%)

  1234 (10,7%)
  1111 (6,0%)
  0000 (1,9%)
  1212 (1,2%)
  7777 (0,7%)

(Stand 2012-10
Quelle: http://www.sueddeutsche.de/wissen/unsichere-pin-codes-erwischt-1.1486312)

Komplexität und Kompetenz.

Security = Kompetenz / Komplexität

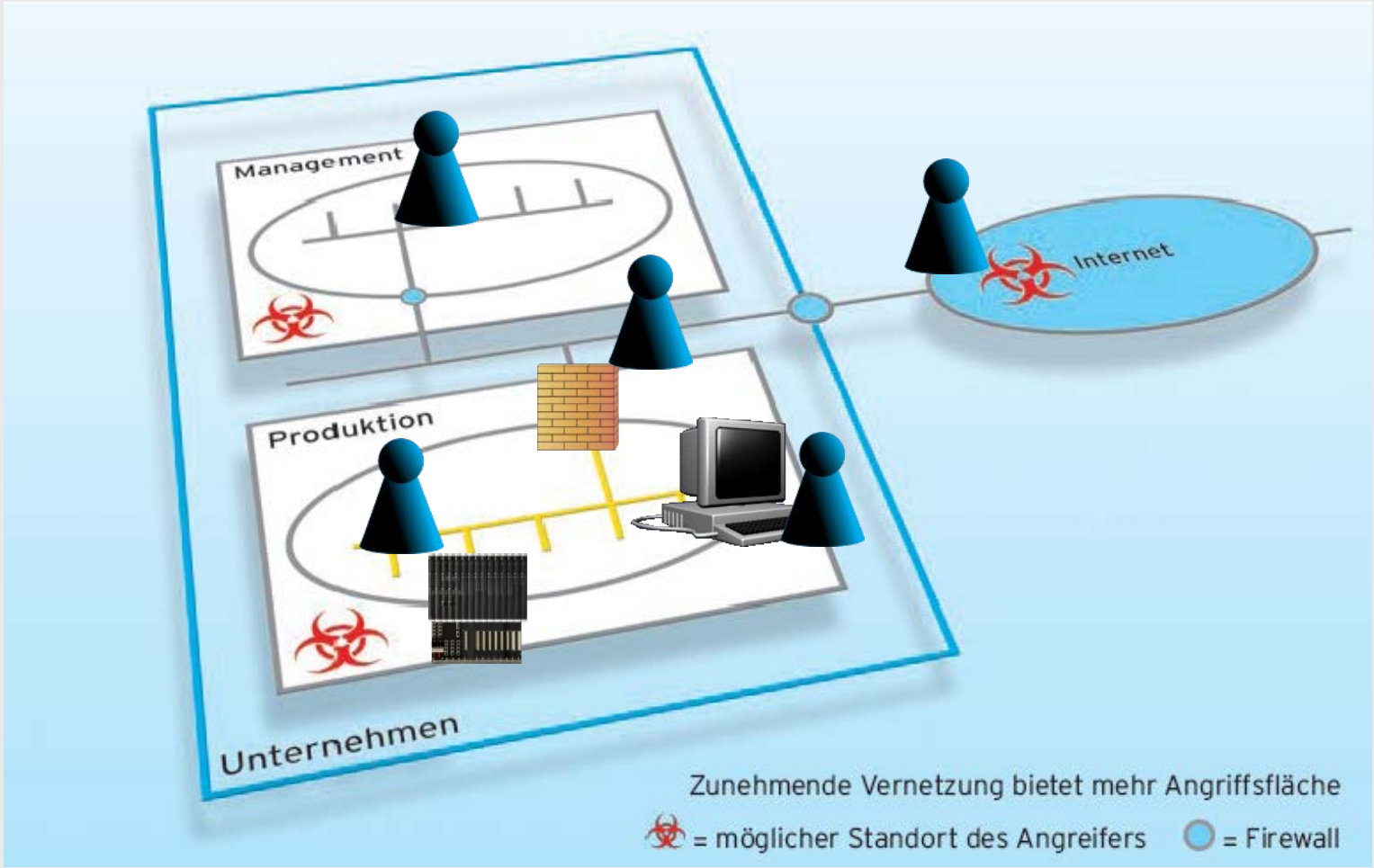


Das sinkende Security Niveau hat einen sinkenden Bedarf an Kompetenz beim Angreifer zur Folge.

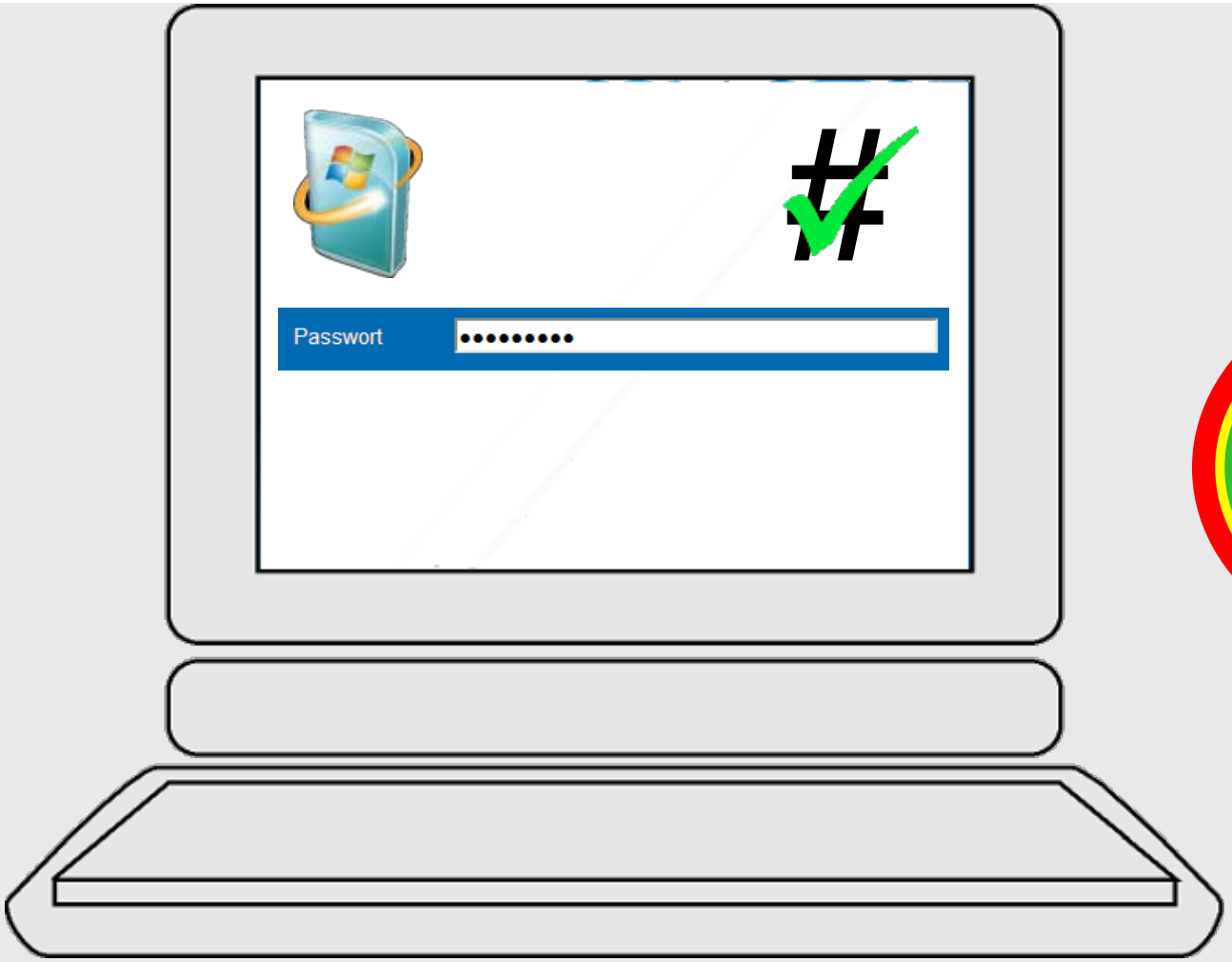
Starten sie ihre Planungen damit das nicht passiert…

Quelle: http://www.dilbert.com/

Umfeld.


Management
Internet
Produktion
Unternehmen
Zunehmende Vernetzung bietet mehr Angriffsfläche
= möglicher Standort des Angreifers
= Firewall

Windows Zutritt.



Passwort £→ #

 # ?→ Passwort

Rainbow Tables

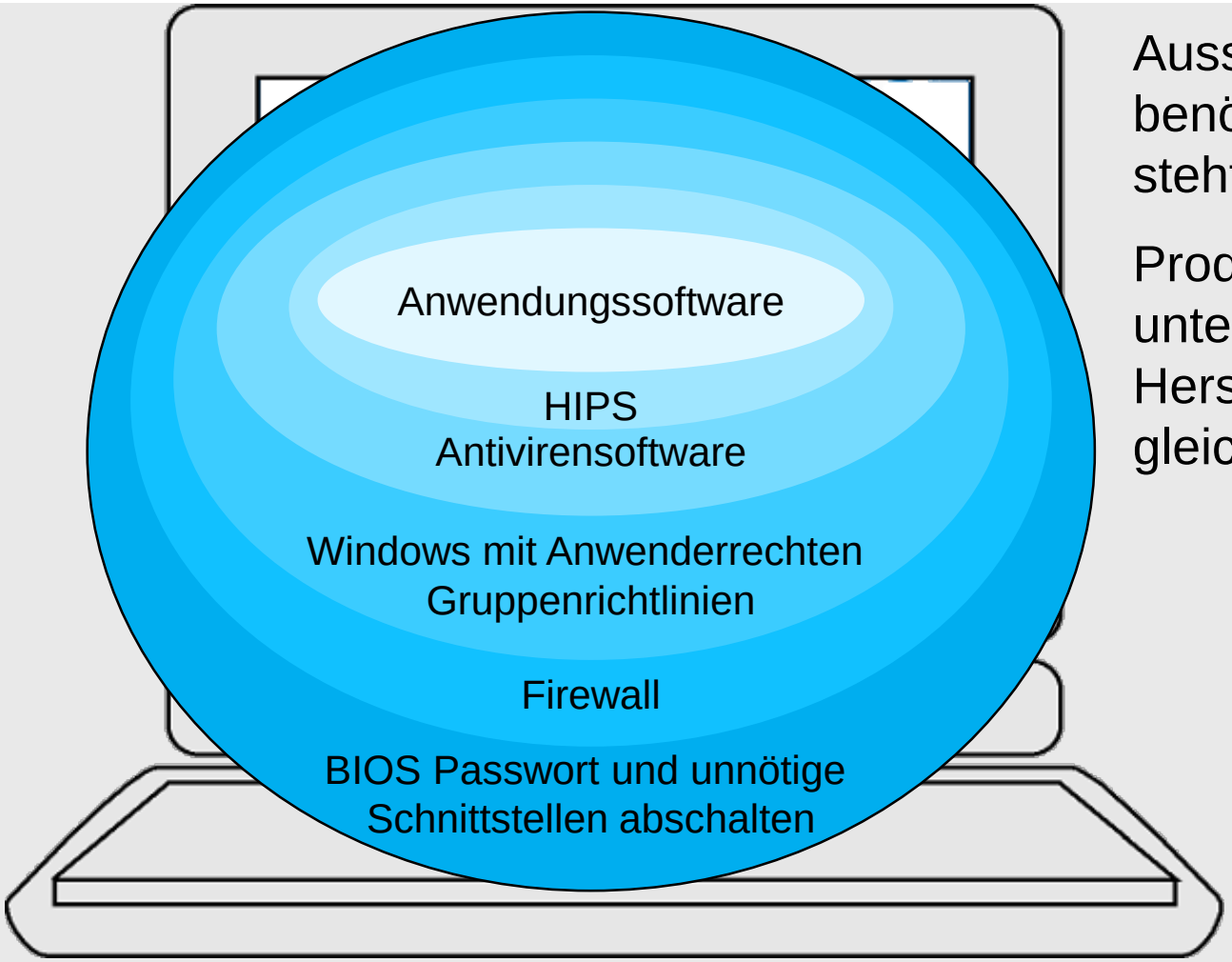
Passwort 1 -> #1

Passwort 2 -> #2

Passwort 3 -> #3

…..

PC-Schutz.



Ausschließlich das was benötigt wird steht zur Verfügung!

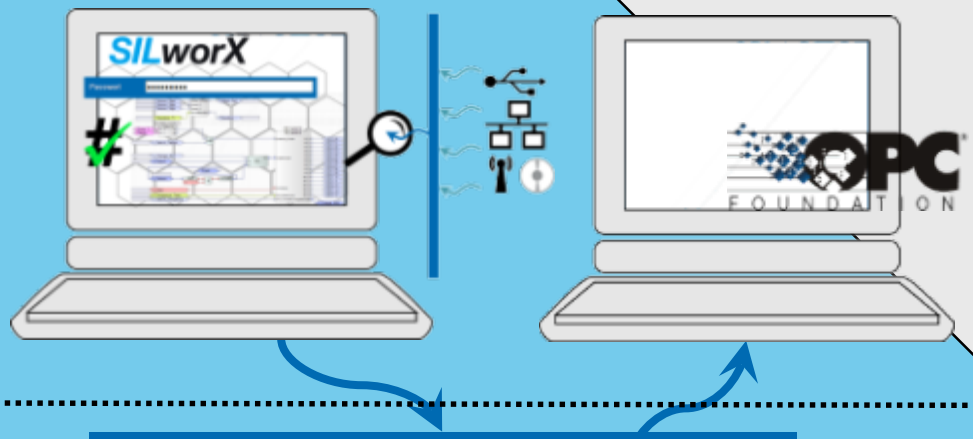
Produkte unterschiedlicher Hersteller vermeiden gleichartige Fehler.

Auch Profis machen Fehler …

Sichere Steuerungen - Security by Design ?!

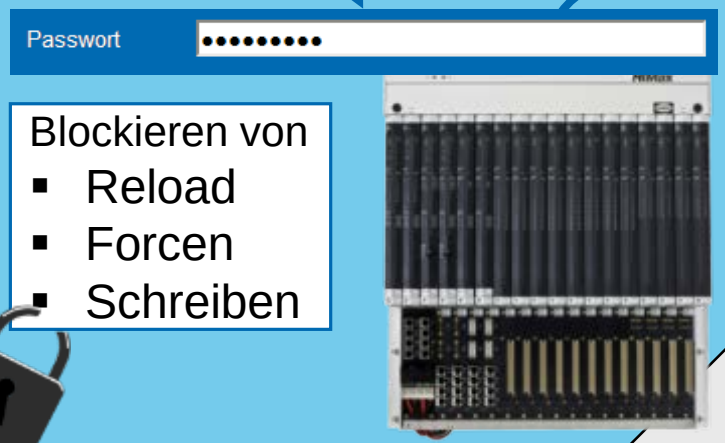
PC

- Windows Minimalkonfiguration
- Einsatz von Schutzsoftware
- Projektschutz…



Steuerung

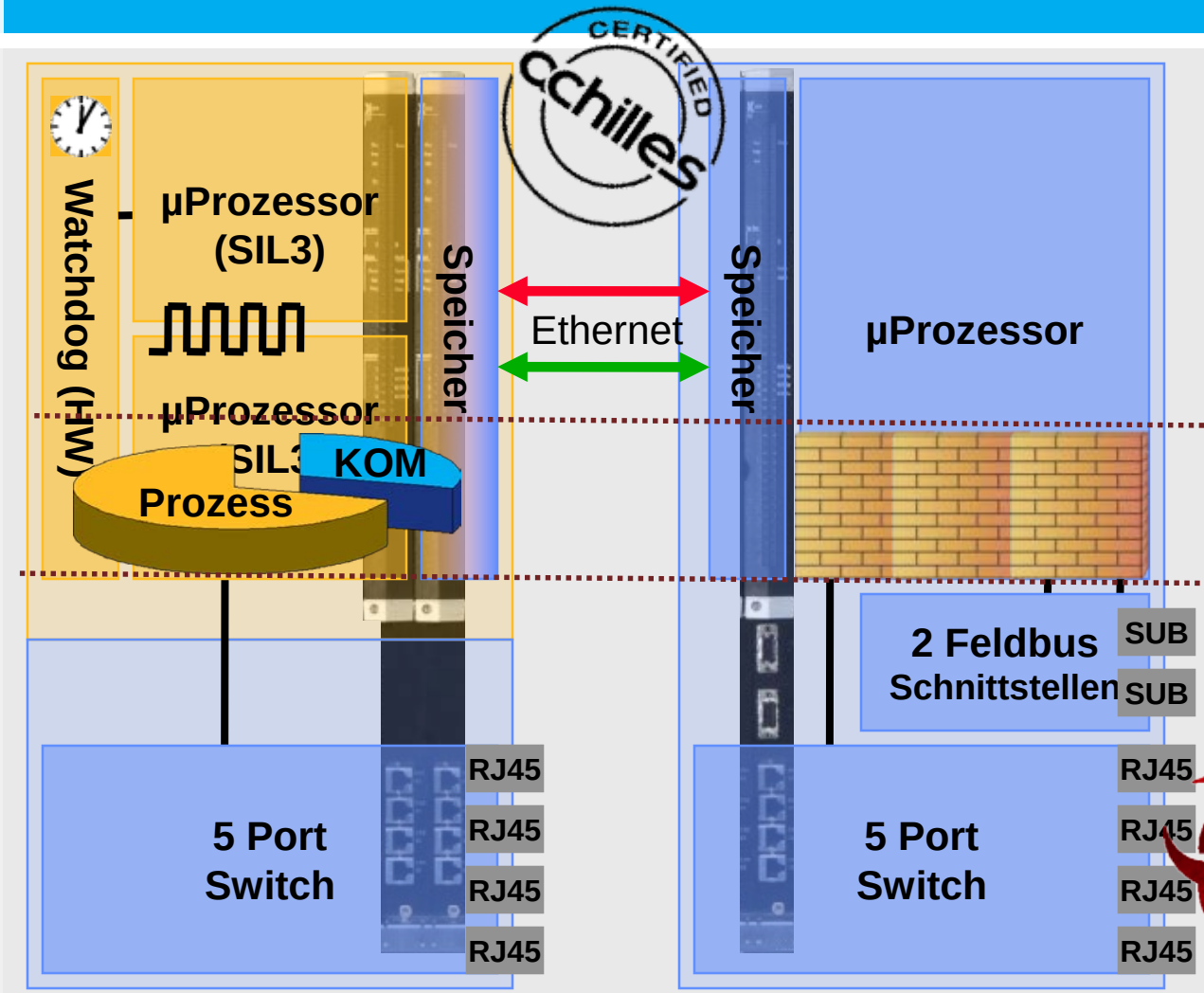
- Systemeinstellungen
- Porteinstellungen
- Protokolle…



Checklisten
→ **systematische Fehler vermeiden !**

Dokumentation VDI 2182

Vollständige Trennung.



- Trennung der Kommunikation vom sicheren Programm.
- Kommunikation wird wie bei einer Firewall auf wenige Ports reduziert.

Zusätzliche technische Maßnahmen...

Modbus

Der Tofino Modbus TCP-Enforcer ermöglicht einen reinen Lesezugriff auf Steuerungen.

Der Honeypot von secXtreme dient dazu nicht geplanten Datenverkehr zu erkennen.

myUSBonly beschränkt die Verwendung von USB sticks.

Windows absichern z.B. mittels Gruppenrichtlinien.

Technische Maßnahmen werden als Ergänzung benötigt.

Fazit.

Etablieren sie technische und organisatorische Maßnahmen.

Security dient keinem Selbstzweck sondern hilft die Grundanforderungen der Automation zu gewährleisten:

- Beherrschbarkeit
- Determinismus
- Safety

Diese ursprünglichen Grundanforderungen sollten in der Euphorie des Featurismus keine Überraschung sein und nicht in Vergessenheit geraten.

Quelle: Wolkig mit Aussicht auf Fleischbällchen

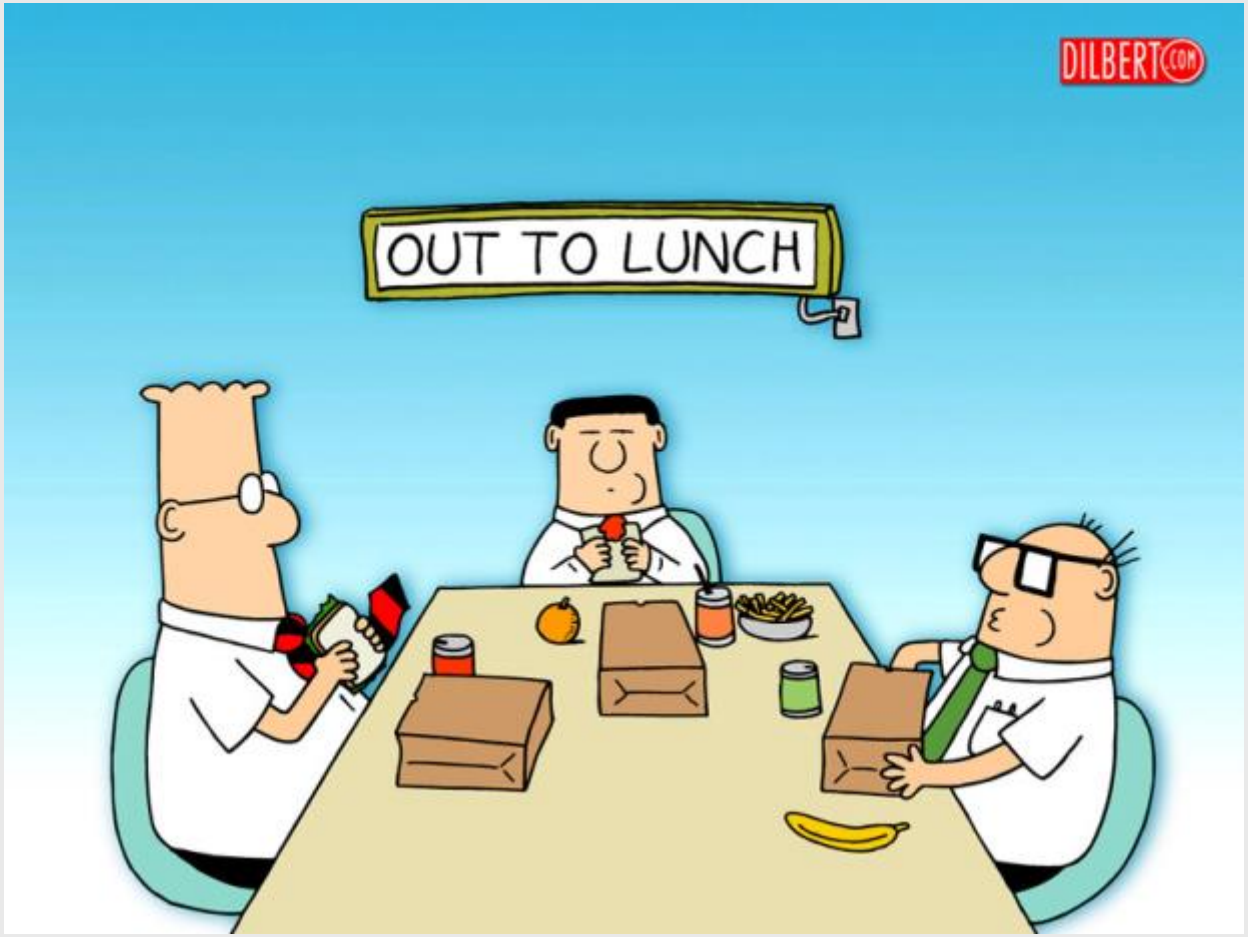
Fragen ?!

Stefan Ditting
Produkt Management
Phone +49 6202 709-426
Fax +49 6202 709-6426
E-Mail: s.ditting@hima.com

http://www.hima.com/Solutions/Integration_solutions/Security_default.php

security@hima.com

Pause.



Quelle: http://www.dilbert.com/


KROHNE
HIMA
SAFETY NONSTOP
PTB
PHOENIX CONTACT
Schneider Electric
FRIATEC
RHEINHÜTTE PUMPEN
TÜV NORD
SAMSON
RITTAL
EPLAN
Medienpartner
P&A
Vielen Dank für Ihre Aufmerksamkeit!